石油炼化

奇安信 新一代网络安全领军者

场景需求 REQUIREMENTS

石油炼化是典型的流程工业生产场景，生产现场控制操作与监测操作主要通过DCS系统实现。当下，炼化企业DCS系统主要以国外品牌为主，系统面临着“设备漏洞缺陷多”，“上位机缺乏安全防护极易感染病毒”，“APC先控系统等关键系统未进行安全防护”等安全风险；另一方面，生产网络的边界缺乏安全防护措施，多使用基于OPC、Modbus等开放、明文通信协议，不具备入侵检测与纵深防御的能力，缺乏实时发现和应对网内的非法访问和恶意攻击，一旦遭到入侵，很可能导致生产运行的瘫痪。

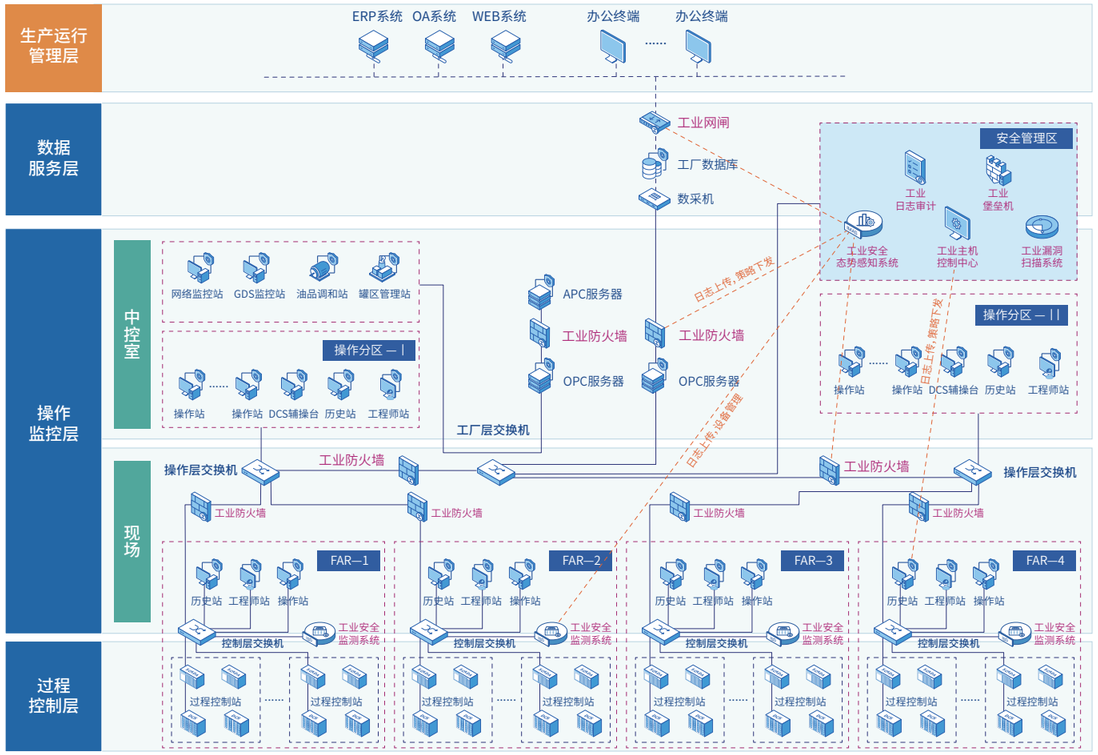
解决方案 SOLUTION

网间域间安全隔离：炼化企业的生产网与办公网之间、生产核心下联不同控制DCS、SIS、PLC等生产控制系统之间、APC先控系统与OPC服务器之间通过部署工业防火墙/网闸类设备进行边界隔离防护。

工控主机安全防护：对DCS、SIS、PLC等控制系统中的操作站主机及数采服务器、MES、APC应用站等重要工控服务器主机部署工业主机防护系统进行主机防护。

网络流量监测审计：对不同装置类别的现场操作间网络的交换机上旁路部署工控网络安全监测系统，自动发现工业资产，洞悉资产脆弱性风险；深入分析网络流量，发现网络内异常操作与入侵行为，及时告警。

安全管理中心：建立炼化工控安全管理区，部署工业安全态势感知平台，对不同装置内的各类安全设备进行统一管理，收集安全数据，基于关联分析引擎、异常行为分析模型，从资产、漏洞、威胁、行为等维度，展示全局网络安全态势。



成功案例 SUCCESSFUL CASE

- 中国石油长庆石化公司
- 中国石油大庆石化公司
- 中国石油大连石化公司
- 泰州石化

油气输送

奇安信 新一代网络安全领军者

场景需求 REQUIREMENTS

油气输送系统作为国家重要的能源基础设施，其担负着将石油天然气由产地输送至需求区域的重要使命，其场景具有”控制点分散，分布范围广“的特点，在监控方面多采用无人值守的方式，普遍使用SCADA系统进行监测与统一调度；SCADA系统由计算机、PLC、RTU等设备组成，部署于首站、分输站、末站和清管站/远控阀室等多个现地业务场景中。在安全建设过程中，应充分考虑控制中心与生产网区域的网络结构与数据流向，依托等保框架，结合潜在安全风险，构建综合防护体系。

解决方案 SOLUTION

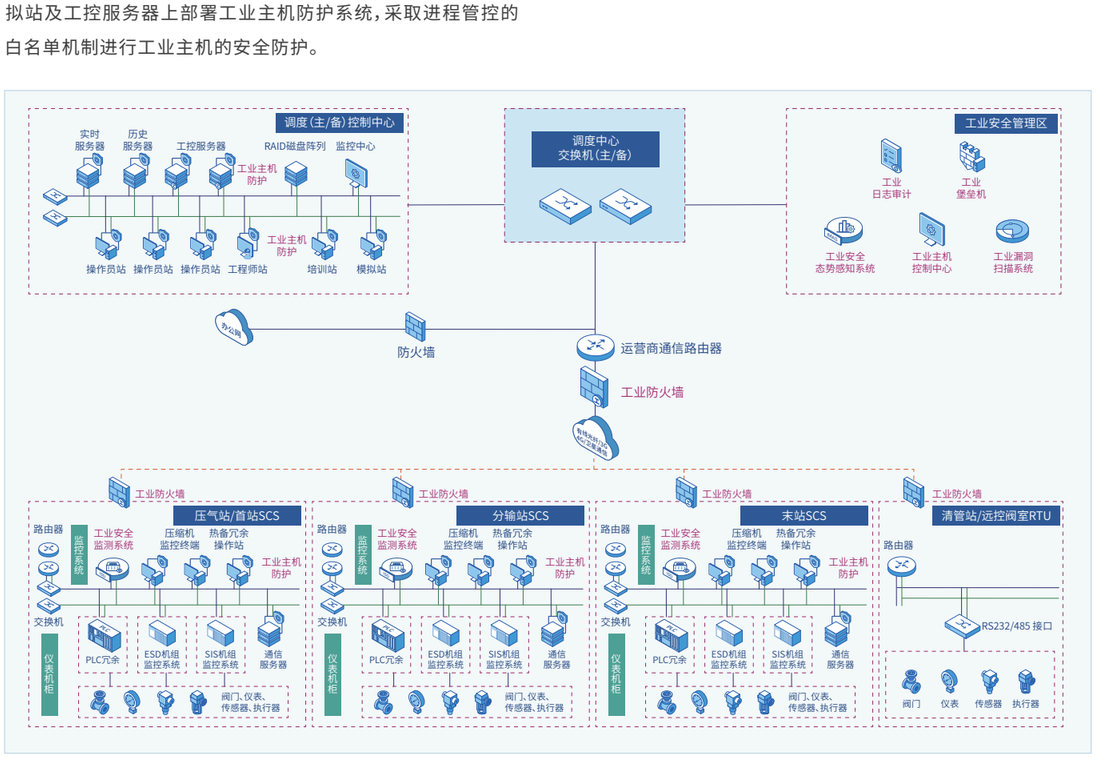
调度中心安全网络边界：在调度中心交换机下联到运营商通信路由器的链路上，从运营商路由器出口到通过有线光纤/3G/4G/卫星通信下联各个场站之间部署工业防火墙，做到对调度中心安全区域的生产网边界防护。

生产区域安全边界：在通过有线光纤/3G/4G/卫星通信链路连接到各个场站的链路上，场站链路边界上部署工业防火墙，实现对场站SCS系统的边界安全防护。

工控主机安全防护：对调度控制中心的工程师站，操作员站，模拟站及工控服务器上部署工业主机防护系统，采取进程管控的白名单机制进行工业主机的安全防护。

生产网安全监测：在首站、分输站、末站的SCS系统内部的网络旁路部署工业安全监测系统，通过端口流量镜像的方式对内网的安全区域进行实施工业安全监测和审计，深入分析网络流量，发现网络内异常操作与入侵行为，及时告警。

安全管理中心：在调度控制中心建立工控安全管理区，部署工业安全态势感知平台，对不同装置内的各类安全设备进行统一管理，收集安全数据，基于关联分析引擎、异常行为分析模型，从资产、漏洞、威胁、行为等维度，展示全局网络安全态势。



成功案例 SUCCESSFUL CASE

- 中国石油廊坊管道公司
- 中国石油昆仑能源公司
- 国家管网北方管道公司